

UNITED STATES DISTRICT COURT
for the
Eastern District of Pennsylvania

In the Matter of the Search of _____
(Briefly describe the property to be searched or identify the person by name and address)
 See Attachment A)
)
)
)
)
)
 Case No. **19-184-M**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*)

See Attachment A.

located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252 and 2252A	Transportation and Possession of Child Pornography

The application is based on these facts:

See attached affidavit, incorporated by reference herein.

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Special Agent Joseph Hartman

Printed name and title

Sworn to before me and signed in my presence.

Date: **2/5/2019**

City and state: Philadelphia, PA


Judge's signature
Honorable Lynne A. Sitarz
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH)

OF:)

)

19-194-m

Google account:)

lorenzomiron2704@gmail.com)

)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Joseph Hartman, being duly sworn, do hereby depose and state:

1. I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered to conduct investigations of, and to make arrests for, the offenses enumerated in Titles 8, 18, 19, 21, 31 United States Code and other related offenses. I am currently employed as a Special Agent with U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI), assigned to the Office of the Special Agent in Charge in Philadelphia, PA. I have been employed as a law enforcement officer since 1998 and have been employed with the HSI and its predecessor, the United States Customs Service, as a Special Agent since 2002. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also

participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses.

2. This investigation involves LORENZO AGUIRRE-MIRON's use of a computer connecting to the internet to transport and possess child pornography, in violation of Title 18, United States Code, §§ 2252 and 2252A.

3. On November 15, 2018, LORENZO AGUIRRE-MIRON was indicted in the Eastern District of Pennsylvania and charged with three counts of manufacturing child pornography, in violation of 18 U.S.C. § 2251(a)(1); one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2); and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). This case was assigned case number 18-521 before the Honorable Judge Eduardo Robreno.

4. After the indictment, I was informed by law enforcement with the Montgomery County Detectives Bureau that they received a National Center for Missing and Exploited Children ("NCMEC") tip that that a Google account held by "Lorenzo Aguirre" using email address lorenzomiron2704@gmail.com, had uploaded child pornography to the cloud storage associated with that Google account.

5. As will be shown below, there is probable cause to believe that fruits, evidence and instrumentalities of the unlawful transportation, receipt and possession of child pornography are located within the Google account registered to lorenzomiron2704@gmail.com. I am submitting this affidavit in support of a search warrant authorizing a search of this email account, which is more particularly described in Attachment A, and the seizure of the items more particularly described in Attachment B.

6. All information contained in this affidavit is either personally known to the affiant or has been related to the affiant by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, U.S.C. §§ 2252 and 2252A, are presently located in the email account lorenzomiron2704@gmail.com.

LEGAL AUTHORITY

7. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, or attempts to do so.

8. Title 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce, or attempts to do so.

9. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Google. I request that Google be required to produce the electronic communications and other information identified in Attachments A and B hereto. Because Google is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Google to perform the search would be a burden upon the company. If all Google is asked to do is produce all the files associated with the account, an employee can do that easily. Requiring Google to search the materials to determine what content is relevant would add to their burden.

10. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B from what is produced by Google pursuant to the search warrant. In reviewing these files, I will treat them in the same way as if I were searching a file cabinet for certain documents. E mails and chat logs will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

11. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

12. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Google to comply even though Google is not located in this district, because the Court has jurisdiction over the offense being investigated.

13. I also ask that the warrant direct Google to produce records and other information pertaining to this account. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth below to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

14. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

DEFINITIONS

15. The following definitions apply to this Affidavit:

- a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the

visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications

equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name -- a user name or screen name, an "email address," an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, email that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that email to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," *see* 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service."

h. An “electronic communications service,” as defined by statute, is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a “remote computing service.” 18 U.S.C. § 2711(2).

i. “Domain names” are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

k. "Uniform Resource Locator or Universal Resource Locator (URL)" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

l. "Spam" email refers to unsolicited (usually commercial) electronic mail messages sent in bulk to recipients.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND E-MAIL

16. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

17. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information.

18. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

19. E-mail is a popular form of transmitting messages and or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

20. Internet-based e-mail is a service provided by an electronic communication service provider allowing individuals to send and receive e-mail from any Internet connected computer, regardless of their location or Internet service provider (ISP). Individuals utilizing Internet-based e-mail services access their accounts by "logging in" through the web-browser software installed on their computer, often by providing an account name and an associated password. Once the service provider's computers have determined the password is correct for the given account name, the individual "logged-in" can access any e-mail sent to their account, and or send e-mail to any other e-mail address accessible via the Internet.

21. Internet-based e-mail service providers reserve and or maintain computer disk storage space on their computer system, usually limited and closely regulated, for the use of the service subscriber for the storage of e-mail communications with other parties, which include graphic files, programs, or other types of date stored in electronic form.

22. Internet-based e-mail service providers maintain records pertaining to the individuals who subscribe to their services. These records could include the account holder's name, address, date of birth, gender, occupation, and the Internet Protocol (IP) address used to establish the account and subsequent accesses to that account.

23. Any e-mail that is sent to a Internet-based e-mail subscriber is stored in the subscriber's "mail box" on the electronic communications service provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the provider's servers indefinitely. Electronic communications service provider's can also perform backups of subscriber's email accounts as routine maintenance in case their servers become inoperable so the content in the subscriber's account is not lost.

24. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the provider's servers, and then transmitted to its end destination. Most Internet-based e-mail users have the option of saving a copy of a sent e-mail. Unless the sender of the e-mail specifically deletes the e-mail from the provider's server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained by the provider, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

25. Internet-based e-mail provider's typically offer services to their subscribers that allow them to store any electronic file (i.e. image files, text files, etc.) on servers maintained and or owned by the provider.

26. E-mails and other electronic files stored on an electronic communications service provider's server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and or other files on the provider's server for which there is insufficient storage space in the subscriber's computer and or which he/she does not wish

to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the provider's server.

27. Gmail is an Internet-based electronic communications system operated by Google. It permits its users to communicate using e-mail through their Gmail service, instant messages, text messages, and group messages through their Hangouts and Voice services, and other social networking type methods. Google also allows its users to use other features such as Google Drive and Google Photos. These are services that users can upload files, to include photos and videos, to be stored in the "cloud" on Google servers and be accessed anywhere from any device as long as they log into their associated Google account. Users can automatically backup their photos and videos from their devices, such as a cell or smart phone, tablet, or computer, into their Google Drive or Photos storage. Users can also set up permissions to only allow themselves to have access to these files or share these files with other specific people.

28. Google also maintains records and history for each Google account. This includes, but is not limited to, data such as Bookmarks, Calendar appointments, Chrome Internet history and searches performed in the Chrome web browser, Location history where the account was accessed from and where device associated with the account was located, Map data to include locations visited and locations searched, and Voice and Audio recordings when using the user's voice to perform searches or other functions on the device the account was accessed from.

NCMEC CYBERTIPLINE

29. The National Center for Missing and Exploited Children ("NCMEC") receives complaints via their CyberTipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These CyberTipline reports are reviewed by a NCMEC analyst and

forwarded to Law Enforcement for further investigation on the information provided in the CyberTipline report. ISPs, ESPs, and others may physically view a picture, video, or any other content that they would then report to NCMEC. Prior to generating the Cybertip, Google did not review this file concurrently to making the report, as historically a person at Google had reviewed a file whose hash (or digital fingerprint) matched the hash of the reported image and determined it contained apparent child pornography.

BACKGROUND OF THE INVESTIGATION

Previous Cybertip

30. On January 30, 2018, NCMEC received information from Google, Cyber tip line Report #27306712, that on between August 19, 2016 and January 29, 2018, LorenzoAguirre948@gmail.com uploaded approximately 119 files containing child pornography. Personnel at Google reviewed the files and determined they contained child pornography before submitting the information to NCMEC's CyberTipline. Along with the report to NCMEC, Google provided subscriber information and connection history for the account along with the images that were transmitted. Based on this NCMEC tip, your affiant conducted extensive investigation which ultimately revealed that LORENZO AGUIRRE-MIRON has manufactured child pornography using a child whom resided in the same home as AGUIRRE-MIRON (hereinafter referred to as Premises A). Two videos and one image of this minor child had been manufactured and uploaded to a Google drive account associated with the Gmail account LorenzoAguirre948@gmail.com. On November 8, 2018, LORENZO AGUIRRE-MIRON was indicted for this criminal activity and charged in 18-521, with three counts of manufacturing child pornography, in violation of 18 U.S.C. § 2251(a)(1); with one count of

receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2); and with one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

31. This matter is scheduled for trial on March 26, 2019 before the Honorable Eduardo Robreno.

Current Cybertip

32. On December 31, 2018, your affiant received information from the Montgomery County Detectives Bureau that NCMEC Cybertip #38201528 reported that Google account lorenzomiron2704@gmail.com had uploaded approximately six images of child pornography to the cloud storage associated with that Google account. The first upload of known hash values containing child pornography occurred on December 15, 2017, with five additional uploads of known hash values containing child pornography occurring on between July 10, 2018 and August 6, 2018.

33. The Cyber tip provided the name “Lorenzo Aguirre” as the user of the Google account and the telephone number (484) 848-4121. The Montgomery County Detectives Bureau discovered that an individual by the name “Lorenzo Aguirre Miron” could be associated with four separate addresses in Norristown, one of which was Premises A.

34. In December 2018, Montgomery Country Detectives attempted to conduct interviews at the four addresses. At the final address in Norristown, Premises A, they interviewed the residents who informed the Detectives that Lorenzo Aguirre, also known as Lorenzo Aguirre-Miron, had resided at the location until he was arrested by Homeland Security Investigations in connection with child pornography.

35. The Montgomery County Detectives confirmed this information with agents at HSI and shared the information of the cyber tip referred to them with HSI.

36. The email address of lorenzomiron2704@gmail.com was unknown by HSI during the original investigation of LORENZO AGUIRRE-MIRON. Further, this Cyber tip was never referred to HSI before being shared by the Montgomery County Detectives Bureau in January 2019.

37. Prior to referring this cyber tip to HSI, the Montgomery County Detective Bureau had not secured a search warrant for Google for the account of lorenzomiron2704@gmail.com.

38. Your Affiant has viewed the images and it is your affiant's opinion that the images associated with the Cyber tip for the account of lorenzomiron2704@gmail.com depict child pornography as defined in 18 U.S.C. § 2256, in that the image files showed prepubescent girls in their underwear or naked and posed in a manner that constitutes lascivious exhibition of the genitals. One image titled "0311120001519592447.jpg" depicts a girl approximately 4-7 years old, with her pants pulled down, exposing her genitalia. The child is posed with her face visible in the photo and she appears to be smirking. The child is posed in a way to elicit sexual arousal.

39. Your affiant has reason to believe that the account of lorenzomiron2704@gmail.com is associated with LORENZO AGUIRRE-MIRON, as the telephone number provided in the NCMEC tip to the Montgomery County Detectives, (484) 848-4121, is a telephone number your affiant has confirmed is the telephone number assigned and utilized by LORENZO AGUIRRE-MIRON prior to his arrest.

40. On October 19, 2018, in response to an Administrative Subpoena, Facebook provided account information related to Lorenzo Aguirre-Miron's Facebook page. LORENZO AGUIRRE-MIRON provided the phone number (484) 848-4121 in connection with his Facebook account.

41. Prior to your affiant being advised of the NCMEC tip sent to Montgomery County Detectives, on October 19, 2018, warrant number 18-1662-M was signed in the Eastern District of Pennsylvania, for location information related to phone number (484) 848-4121, assigned to T-Mobile and used by LORENZO AGUIRRE-MIRON. Pursuant to this warrant, T-Mobile provided location information to law enforcement that indicated that LORENZO AGUIRRE-MIRON was believed to be located inside of Premises A.

42. LORENZO AGUIRRE-MIRON was subsequently arrested at Premises A on October 19, 2018 and ultimately indicted on November 8, 2018. The phone bearing (484) 848-4121 was confiscated from LORENZO AGUIRRE-MIRON at the time of his arrest.

CONCLUSION

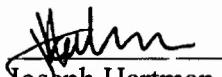
43. Based on the aforementioned information, your Affiant respectfully submits that there is probable cause to believe that the Google account registered to lorenzomiron2704@gmail.com has transported and possessed child pornography, that is, visual depictions of minors engaging in sexually explicit conduct, or attempted to do so, and respectfully submits that there is probable cause to believe the account and other computer servers of Google located at or maintained by Google, 1600 Amphitheater Parkway, Mountain View, California, contain evidence of the violations of Title 18, United States Code, Sections 2252 and 2252A.

44. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachments A and B.

45. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrant, this

affidavit in support of application for search warrant, the application for search warrant and all attachments thereto, and all related docket entries be filed under seal until further order of this Court. For this same reason, I request that the Court issue an order under 18 U.S.C. § 2705(b) precluding Google from giving notice to the customer

Respectfully submitted,


Joseph Hartman
Special Agent
Homeland Security Investigations

Subscribed and sworn before me
this day 5th of February, 2019.


HONORABLE LYNNE A. SITARSKI
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the accounts registered to
lorenzomiron2704@gmail.com which are stored at premises owned, maintained, controlled, or
operated by Google LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain
View, California 94043.

ATTACHMENT B-1

Particular Things to be Seized

- I. Information to be disclosed by Google, Inc.**
- A. All account information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, services and apps used, and other personal identifiers; buddy lists, contacts, and address books;
 - B. All communications and messages made or received by the user to include e-mails (read, sent, deleted, draft, and unopened) whether in a mailbox, user created folders, or other storage locations, attachments, documents, graphics, and any other uploaded, saved, or associated files, including all messages in Hangouts or Voice whether active, deleted, or archived;
 - C. All content in the user's Google Drive online storage along with any settings on who has access to the files or folders and dates, times, and IP address of when the files were uploaded;
 - D. All content in the user's Google and Google + Photos, to include all albums, photos, videos, and metadata for each file, as well as all storage and backup files, Contents of all Google+ posts and/or comments associated with the account, as well as a copy of the Google+ profile and the Google+ circles and contacts;
 - E. All logs showing the devices used to log into the accounts and checkins for those devices that show the IP address, date/time, make and model of the device, and SIM operator;
 - F. All Bookmarks, Calendar, Chrome data to include searches and browser history, all Location history, all Maps history to show searches and places visited, all Google search

history, all Web and App activity, Devices used to access the accounts, and all Voice and Audio activity to include any voice recordings;

- G. All activity logs and IP logs, including all records of the IP addresses that logged into the account;
- H. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
- I. All privacy settings and other account settings;
- J. All records pertaining to communications between Google and any person regarding the user or the user's Google account, including contacts with support services and records of actions taken;
- K. Notwithstanding Title 18, United States Code, Sections 2252 and 2252A, Google shall disclose responsive data, if any, by delivering encrypted files through Google's Law Enforcement Request System (LERS).
- L. The data listed above in paragraphs A through K shall be produced by Google regardless of where it may be stored.

ATTACHMENT B-2

(To be executed by Law Enforcement Agents)

Items to be seized:

Evidence of the violations of 18 U.S.C. §§ 2252 and 2252A, as follows:

- A. All files, documents, communications, images, videos, logs, and contacts associated with the Google account lorenzomiron2704@gmail.com related to visual depictions of minors engaging in sexually explicit conduct or child pornography, in violation of Title 18 U.S.C. Sections 2252 and 2252A, along with any evidence that would tend to show the true identities of the persons committing these offenses, the identities of the persons depicted in the images, videos, or other files, or the identities of the persons distributing or receiving the images, videos, or other files.
- B. All activity logs and IP logs, including all records of the IP addresses that logged into the account.
- C. All account information, including:
 - a. All account information, including: full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, services and apps used, downloaded, or purchased, and other personal identifiers; buddy lists, contacts, and address books;
 - b. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);
 - c. All privacy settings and other account settings;
 - d. All logs of devices and accompanying serial or model numbers and other

identifying numbers to include dates of activation, registration,

deactivation, or use;

e. All logs showing the location of the user;

f. All records pertaining to communications between Google LLC and any person regarding the user or the user's Google accounts, including contacts with support services and records of actions taken; and

g. All records that tend to show the true identity or location of the user of these accounts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature